CIPHERMAIL EMAIL ENCRYPTION

Ciphermail for BlackBerry Reference Guide

June 19, 2014, Rev: 8975

Contents

1 Introduction

The BlackBerry smartphone is the most secure generally available smartphone on the market. All communication between a BlackBerry Enterprise Server (BES) and a BlackBerry smartphone is encrypted with 3DES or AES. For added security the S/MIME support package can be installed allowing email to be digitally signed and encrypted using digital certificates.

BlackBerry Internet Service (BIS) users however, do not have the same level of protection that BES users have. Even though all communication between the carriers BIS and a BlackBerry smartphone is encrypted, data from the carriers BIS to the Internet is not. Email sent to and from a BlackBerry smartphone goes without any protection and can potentially be intercepted and/or modified by any intermediate gateway.

Ciphermail for BlackBerry can be used to send and receive S/MIME digitally signed and encrypted email from a BlackBerry smartphone. Ciphermail for BlackBerry is an add-on to the built-in BlackBerry mail application and is used in combination with the Ciphermail Email Encryption Gateway[1].

The most difficult part of email encryption is key management. This is especially hard on mobile devices. Ciphermail for BlackBerry therefore relies on the Ciphermail gateway for most certificate management functions. Because all email is automatically encrypted with S/MIME, all email in transit and at rest is protected against unauthorized access.

Ciphermail for BlackBerry is most beneficial to BIS users because BIS does not natively provide point-to-point encryption. BES users however can benefit from Ciphermail for BlackBerry as well. Because all incoming and outgoing email is automatically S/MIME encrypted without requiring any user intervention, a high level of protection is guaranteed. This can be helpful when the organization hosting the BES is not fully trusted (for example the BES is hosted externally).

2 BlackBerry add-on

Ciphermail for BlackBerry is a BlackBerry application that integrates with the built-in BlackBerry mail application.

Features: Ciphermail for BlackBerry has the following features:

- S/MIME encryption and digital signing using X.509 certificates.
- Compatible with BIS.
- Compatible with existing S/MIME clients (like Outlook and Lotus Notes).
- Message body and attachments are encrypted.
- HTML email support.
- Uses BlackBerry encryption functionality (3DES, AES, X.509, S/MIME).

[1] If sending of encrypted email from a BlackBerry smartphone is not required, any email server capable of rewriting headers can be used (see Appendix A for more info)

- Uses the BlackBerry built-in key and certificate store.
- Compatible with the BlackBerry smart card reader.
- Encrypted messages sent from BlackBerry smartphone are securely relayed by the Ciphermail gateway via an encrypted S/MIME tunnel.
- Because email is relayed by the Ciphermail gateway, email sent from the BlackBerry can be easily archived using any existing email archiving functionality.
- Messages are stored on the BlackBerry smartphone in encrypted form.
- Because email is relayed by the Ciphermail gateway, all email originates from the companies IP range. This is especially useful when the companies domains have SPF records setup.

Receiving S/MIME encrypted email Ciphermail email encryption gateway can be setup to automatically encrypt all email sent to the BlackBerry user (see figure 1). Messages which are already S/MIME encrypted, for example the message has been encrypted with Outlook, are relayed in encrypted form to the BlackBerry user.

Whether or not the message is automatically decrypted after the user opens the message depends on the size of the encrypted message. Messages larger than 64KB are not automatically delivered to the BlackBerry smartphone and should be manually downloaded by the user[2].

S/MIME message require some changes to the headers to prevent BIS from blocking the S/MIME message. See Appendix A for more information on how BIS handles attachments and why S/MIME message headers must be rewritten.

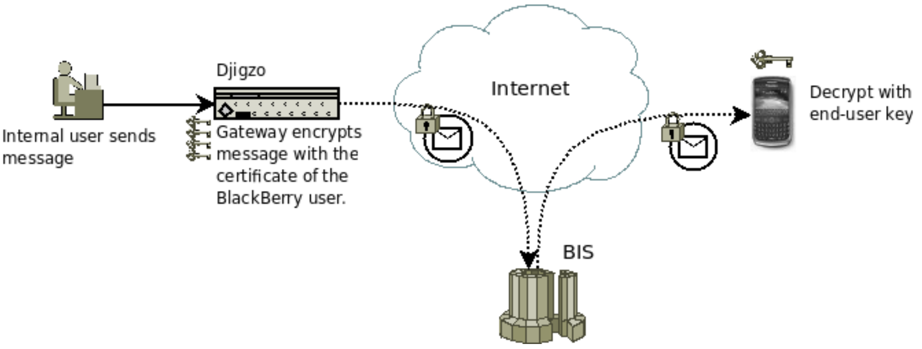

Internal user sends message
Djigzo
Gateway encrypts message with the certificate of the BlackBerry user.
Internet
BIS
Decrypt with end-user key

Figure 1: Receiving encrypted email on a BlackBerry. The internal user sends a message to an external user. The message is encrypted by the Ciphermail gateway using the certificate of the BlackBerry user. The message is decrypted with the users private key on the BlackBerry when the user opens the message.

[2] The message headers are directly delivered but the encrypted content is not. The user should manually open the attachment. Downloading large messages on demand instead of sending them directly saves bandwidth.

Sending S/MIME encrypted email The most difficult part of email encryption is key management. Selecting the correct certificate for a recipient, importing root certificates etc. requires some knowledge of the PKI process. This is especially hard on a mobile device.

Ciphermail for BlackBerry therefore relies on the Ciphermail gateway for most of the certificate management functions. Messages sent from a BlackBerry smartphone with Ciphermail for BlackBerry are encrypted with a server certificate and digitally signed with the BlackBerry users personal certificate. The Ciphermail gateway checks whether the sender is allowed to relay messages through the Ciphermail gateway and whether the digital signature is correct. Only if the signature is correct and the message is signed with the correct private key, will the message be forwarded to the final recipient (see figure 2). Whether or not messages sent to the final recipients are encrypted by the Ciphermail gateway depends on the gateway settings.

All messages sent from the BlackBerry smartphone with Ciphermail for BlackBerry are digitally signed. The digital signature is used to authenticate the BlackBerry user. Only users with an approved private key will be allowed to sent email via the Ciphermail gateway.

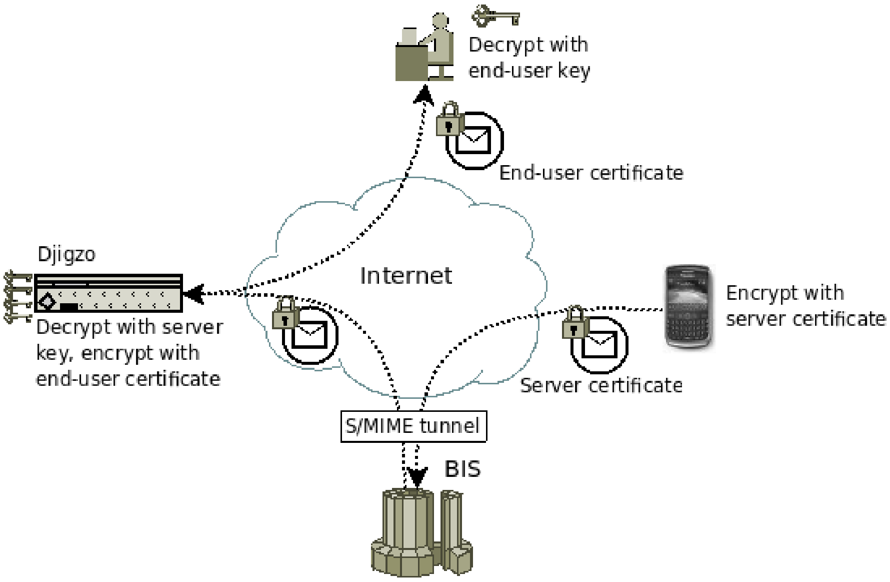


Figure 2: Sending encrypted email from a BlackBerry. The BlackBerry user sends a message. The message is digitally signed with the senders private key, then encrypted with the server certificate and sent to the Ciphermail gateway. The Ciphermail gateway decrypts the message and checks the signature. The message is then sent to the final recipient encrypted with the recipients certificate.

2.1 Installation

Ciphermail for BlackBerry is a BlackBerry application which can be installed on a BlackBerry smartphone. Ciphermail for BlackBerry can be installed overthe-air from http://m.ciphermail.com/bb. There are different versions for different BlackBerry OS versions: 4.5, 4.6 and $\geq$ 4.7.

Alternatively Ciphermail for BlackBerry can be downloaded on a desktop and installed with the BlackBerry desktop manager.

2.2 Import certificate and key

Ciphermail for BlackBerry requires an X.509 certificate with a private key to be available on the BlackBerry smartphone. A certificate and key can be imported onto the BlackBerry smartphone using the BlackBerry Desktop Manager.

2.2.1 Import certificate and key into Windows

Before a certificate and key can be imported into the BlackBerry smartphone, the desktop system on which the BlackBerry Desktop Manager is running should contain the correct certificate and key. There are different ways a BlackBerry user can get a certificate and key. One option is to use one of the available commercial certificate vendors like Verisign, Comodo etc. A secure and more practical option is to use Ciphermail's built-in CA functionality. With the built-in CA a certificate and key can be generated for the BlackBerry user (see the Ciphermail Administration Guide for more information). The certificate and key should be imported into the desktop system by double clicking the .pfx file (see Appendix B for instructions on importing a .pfx into Windows).

2.2.2 Import certificate and key into BlackBerry

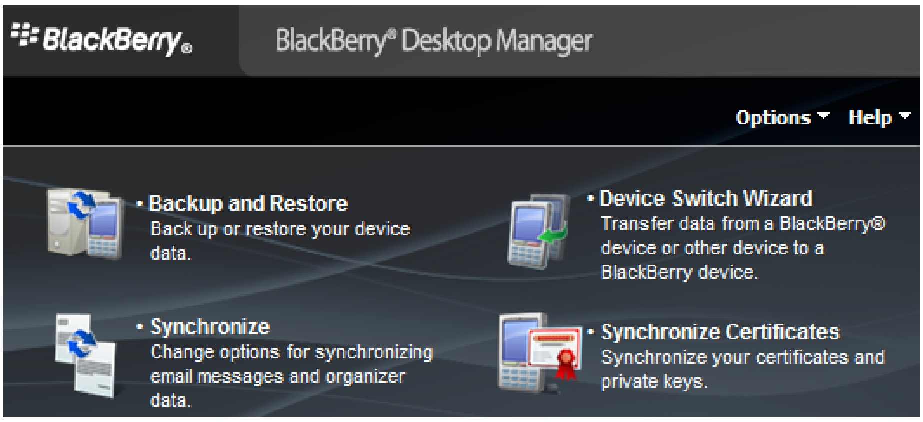
The certificate and the key should be imported onto the BlackBerry smartphone using the BlackBerry Desktop Manager Certificate Synchronization tool (see "Synchronize Certificates" in figure 3). If the Synchronize Certificates option is not available it should be enabled first.

Enable Certificate Synchronization option This paragraph can be skipped if the Synchronize Certificates option is already enabled. The Synchronize Certificates option can be enabled by modifying the BlackBerry Desktop Software.

On Windows, open the Control Panel → Add or Remove Programs → Select BlackBerry Desktop Software and click the Change/Remove button. This opens the BlackBerry Desktop Software installation wizard. Enable the "Certificate Synchronization" option and finish the wizard by pressing Next and Finish (see figure 4).

Certificates can be imported onto the BlackBerry smartphone by connecting the BlackBerry smartphone to the desktop and clicking "Synchronize Certificate" (see figure 3). The first time certificates and keys are synchronized, a new Key Store Password must be set. The Key Store stores private keys, it is password protected. After you entered the password, the Certificate Synchronization tool is started (see figure 5).

The BlackBerry Synchronization tool synchronizes the Windows certificate and key stores with the BlackBerry certificate and key stores. The Synchronization tool has multiple tabs: Personal certificates, Other people's certifi-



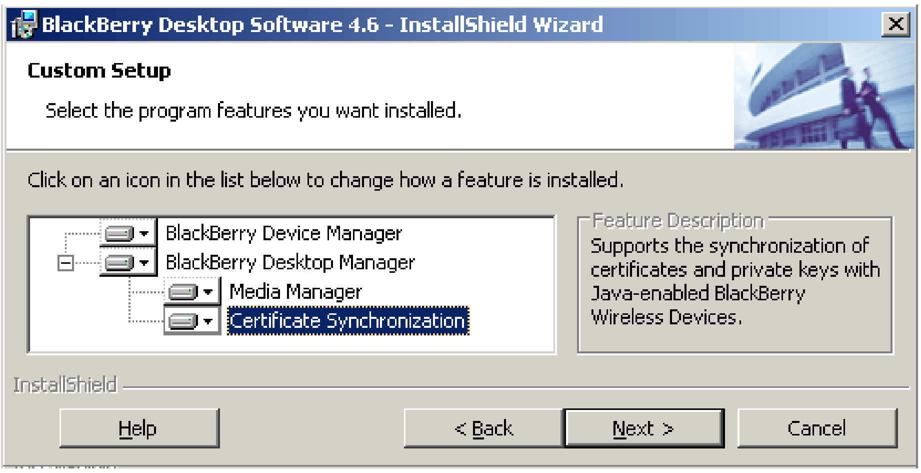
Backup and Restore
Back up or restore your device data.

Device Switch Wizard
Transfer data from a BlackBerry® device or other device to a BlackBerry device.

Synchronize
Change options for synchronizing email messages and organizer data.

Synchronize Certificates
Synchronize your certificates and private keys.

Figure 3: BlackBerry Desktop Manager



Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

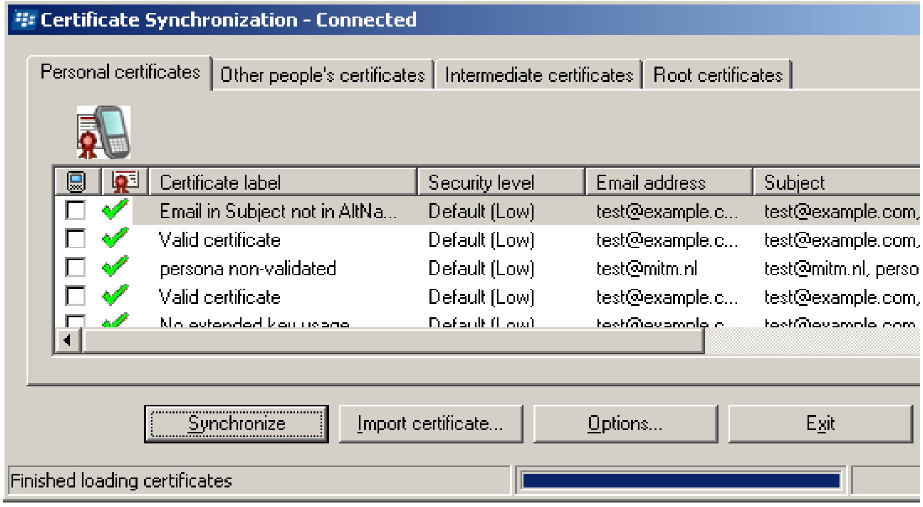
- BlackBerry Device Manager
- BlackBerry Desktop Manager
  - Media Manager
  - Certificate Synchronization

Feature Description
Supports the synchronization of certificates and private keys with Java-enabled BlackBerry Wireless Devices.

Figure 4: Enable Certificate Synchronization option

cates, Intermediate certificates and Root certificates. Ciphermail for BlackBerry requires a certificate with an associated private key. Therefore you must synchronize the certificates and keys in the “Personal certificates” store. The certificates and keys from the Personal certificate store can be synchronized by selecting the checkboxes for all the required certificates and then click “Synchronize”.

Certificate synchronization options Import options can be set on the Certificate synchronization options page which can be opened by clicking “Options”. The *Private key security level* option is relevant for Ciphermail for BlackBerry. If the Private key security level is set to *Medium* or *High* a password must be entered when the private key is accessed. With the *High* security level, a password must be entered every time the private key is accessed. With


Certificate Synchronization - Connected
Personal certificates
Other people's certificates
Intermediate certificates
Root certificates
Synchronize
Import certificate...
Options...
Exit

		Certificate label	Security level	Email address	Subject
□	✓	Email in Subject not in AltNa...	Default (Low)	test@example.c...	test@example.com,
□	✓	Valid certificate	Default (Low)	test@example.c...	test@example.com,
□	✓	persona non-validated	Default (Low)	test@mitm.nl	test@mitm.nl, perso
□	✓	Valid certificate	Default (Low)	test@example.c...	test@example.com,
□	✓	No extended key usage	Default (Low)	test@example.c...	test@example.com

Finished loading certificates

Figure 5: Certificate Synchronization tool

the *Medium* security level the key store password is cached for some time[3]. With the *Low* security level, a password is not required when the private key is accessed. The *Low* security level should only be used if the BlackBerry smartphone is password protected.

You can change the Private key security level after import with the "Change Security Level" menu item in the certificate settings screen.

2.3 Configuration

After Ciphermail for BlackBerry has been installed and the certificates and private keys have been imported into the BlackBerry smartphone, Ciphermail for BlackBerry should be configured. The configuration screen can be opened by clicking the Ciphermail icon in the download folder[4] (see figure 7).

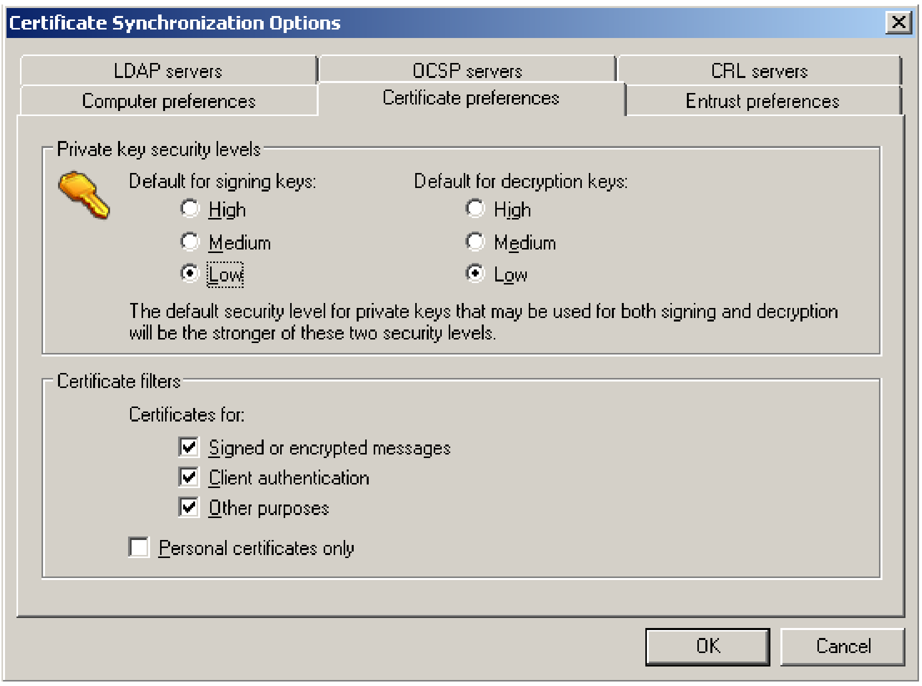
2.3.1 Settings

On the Ciphermail settings screen the following settings can be configured: *From*, *Reply-To*, *Sign cert*, *Enc. cert*, *Relay email*, *Enc. trigger*, *Show Send Encrypted*, *Show Send PDF/SMS*, *Add Sig. Line* and *Show advanced*(see figure 8).

From When a relay message if forwarded by the gateway, the *From* header of the new message will be set to this value. Whether or not a specific From is allowed is determined by the Ciphermail gateway settings. The default From value will be set to the BlackBerry default email address. This setting is only used when sending encrypted email from the BlackBerry smartphone.

[3] The password timeout can be set in Advanced Security Options → Key Stores. See the option *Private Key Password Timeout*

[4] By default, newly installed applications are stored in the download folder.



Private key security levels

Default for signing keys:
○ High
○ Medium
● Low

Default for decryption keys:
○ High
○ Medium
● Low

The default security level for private keys that may be used for both signing and decryption will be the stronger of these two security levels.

Certificate filters

Certificates for:
☑ Signed or encrypted messages
☑ Client authentication
☑ Other purposes

□ Personal certificates only

Figure 6: Certificate synchronization options

Reply-To When a relay message if forwarded by the gateway, the *Reply-To* header of the new message will be set to this value. If the Reply-To is not specified, replies will be sent to the sender (i.e. to the From email address). This setting is only used when sending encrypted email from the BlackBerry smartphone.

Signing certificate (*Sign cert*) The signing certificate is the certificate which is used for digitally signing outgoing messages (to be precise, the private key associated with the certificate is used for signing). The signing certificate is used to authenticate the sender of the message. Only if the message is signed with the correct private key will be sender be allowed to relay email through the Ciphermail gateway.

A signing certificate can be selected by pressing the "..." button. Select the correct signing certificate from the popup screen.

Because a private key is required for signing, only certificates with an associated private key can be selected. The selected signing certificate should be the certificate selected as the users *Relay certificate* (see *Relay certificates* setting of the Ciphermail gateway at page 27). A warning will be shown if there are no suitable certificates available. This setting is only used when sending encrypted email from the BlackBerry smartphone.

Encryption certificate (*Enc. cert*) Email sent from the BlackBerry smartphone must be encrypted with a certificate for which the Ciphermail gateway has a private key (the Ciphermail gateway should be able to decrypt the mes-

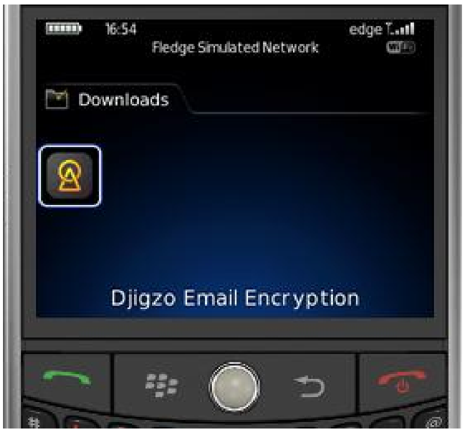
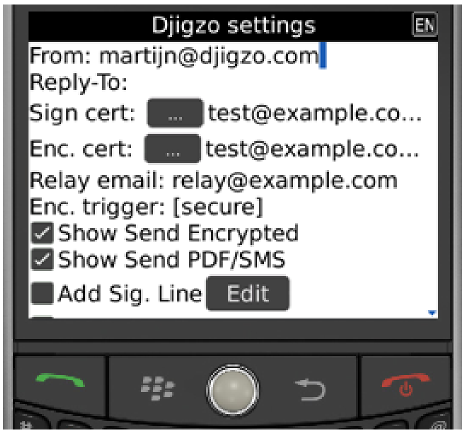


Figure 7: Ciphermail Settings Icon



Djigzo settings EN

From: martijn@djigzo.com
Reply-To:
Sign cert: ... test@example.co...
Enc. cert: ... test@example.co...
Relay email: relay@example.com
Enc. trigger: [secure]
☑ Show Send Encrypted
☑ Show Send PDF/SMS
□ Add Sig. Line Edit

Figure 8: Ciphermail Settings

sage). The Encryption certificate will be used to encrypt all email sent from the BlackBerry smartphone (via an S/MIME tunnel).

An encryption certificate can be selected by pressing the "..." button. A warning will be shown if there are no suitable certificates available. This setting is only used when sending encrypted email from the BlackBerry smartphone.

Relay email When sending encrypted email with Ciphermail for BlackBerry, the email is securely relayed through the Ciphermail gateway via an encrypted S/MIME tunnel.

The Relay email address setting is the email address that the Ciphermail gateway uses for incoming relay messages. The Relay email address setting should be equal to the *Relay email* setting of the Ciphermail gateway (see *Relay email* setting of the Ciphermail gateway at page 28 for more information). This setting is only used when sending encrypted email from the BlackBerry smartphone.

Encryption trigger (*Enc. trigger*) The Ciphermail gateway can be setup to allow a specific keyword in the subject of the message to trigger encryption (see the Ciphermail Administration Guide for more information). The Encryption trigger setting specifies the keyword which will be added to the subject when a messages is sent using the *Send Encrypted* menu option.

The encryption trigger is used if the BlackBerry sender wants to be certain that email relayed by the Ciphermail gateway is encrypted when forwarded to the final recipient. See the Ciphermail Administration Guide for more information on the Subject trigger setting. This setting is only used when sending encrypted email from the BlackBerry smartphone.

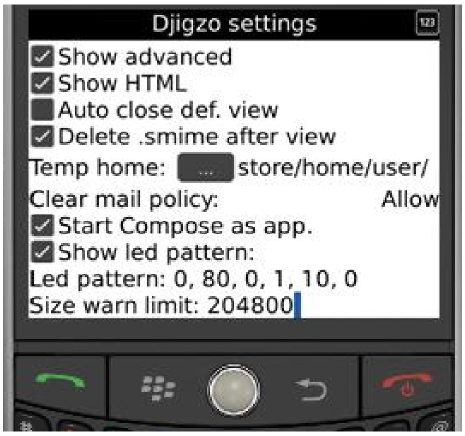
Show Send Encrypted If checked, the *Send Encrypted* menu option will be shown in the secure email compose screen. Uncheck this option if the user is not allowed to trigger encryption with a subject trigger (see *Enc. trigger* setting).

Show Send PDF/SMS If checked, the *Send PDF/SMS* menu option will be shown in the secure email compose screen. Uncheck this option if the user is not allowed to send SMS Text message from the Ciphermail gateway (see the Ciphermail Administration Guide for more information).

Add Signature Line (*Add Sig. Line*) If checked, a signature line will be appended to the message body when a new email is composed. The signature content can be edited by clicking the “Edit” button. This setting is only used when sending encrypted email from the BlackBerry smartphone.

2.3.2 Advanced settings

Advanced settings can be edited by selecting the “Show advanced” checkbox (see figure 9).



Djigzo settings

☑ Show advanced
☑ Show HTML
□ Auto close def. view
☑ Delete .smime after view
Temp home: ... store/home/user/
Clear mail policy: Allow
☑ Start Compose as app.
☑ Show led pattern:
Led pattern: 0, 80, 0, 1, 10, 0
Size warn limit: 204800

Figure 9: Ciphermail advanced settings

The following advanced settings can be set: *Show HTML*, *Auto close def. view*, *Delete .smime after view*, *Temp home*, *Clear mail policy*, *Base URL workaround*, *Start Compose as app.*, *Show led pattern*, *Led pattern* and *Size warn limit*.

Show HTML Sometimes a message contains a text part and an alternative HTML part. If the *Show HTML* option is checked, the HTML part will be shown by default. The *Text Mode* menu option can be used to switch to the text part. If Show HTML is not checked, the text part will be shown by default. This setting is only used for reading encrypted email on the BlackBerry smartphone.

Auto close default view (*Auto close def. view*) If selected, the default message view will be closed after viewing the S/MIME message. If not selected the message containing the encrypted *smime.p7m* attachment will be shown when the S/MIME message view is closed. By default *Auto close def. view* is selected.

Delete .smime after view When an S/MIME message is larger than 64KB, the S/MIME message is not immediately delivered to the BlackBerry smartphone (see appendix A for more information). The user has to manually open the S/MIME message by selecting *Open Attachment* from the context menu. The S/MIME message will be downloaded as a *.smime* file and saved to a temporary location (see the *Temp home* setting).

If *Delete .smime after view* is checked, the downloaded *.smime* file will be deleted after the message has been opened. Leave this value checked unless there are compelling reasons to keep the downloaded *.smime* files. If a downloaded message should be saved, select the *Save Message* context menu item after the message has been opened. This setting is only used for reading encrypted email on the BlackBerry smartphone.

Temp home The Temp home setting specifies the location where temporary files will be stored. For example if an encrypted message has an attachment and the user opens the attachment by clicking it, the attachment will be extracted to the temporary directory. The directory which stores the temporary files will be periodically cleaned with a *Memory Cleaner*[5].

The default value of *Temp home* will be set to the users home directory (store/home/user). Leave the default value unless there are compelling reasons to change it. This setting is only used for reading encrypted email on the BlackBerry smartphone.

Clear mail policy *Clear mail policy* determines what happens when the user composes a non secure email (i.e. an email which is not relayed via the S/MIME tunnel to a Ciphermail gateway). The following policies are available: *Allow*, *Warn* and *Deny*.

[5] The Ciphermail memory cleaner automatically cleans the temporary directory when the BlackBerry is holstered, idle etc. (see advanced security options → Memory Cleaning).

The Allow policy allows the user to create a non-secured email, the Warn policy allows the user to create a non-secured email but a warning will be shown and the Deny policy won't allow the user to compose a non-secured email. This setting is only used when sending encrypted email from the BlackBerry smartphone.

Start Compose as app. This setting enables a workaround for a bug in OS 4.6.1 on 8900. Enable this option when the compose secure email screen is extremely sluggish. This setting is only used when sending encrypted email from the BlackBerry smartphone.

Show led pattern If enabled, the LED will blink with the given *Led pattern* when decrypting or encrypting email. This is used to notify the user that an email is being encrypted or decrypted.

Led pattern The LED blink pattern used when encrypting or decrypting a message (see *Show led pattern*). The LED pattern is string consisting of color/duration/transition tuples. The color is the RGB color (0-FFFFFF), the duration is the duration in milliseconds for this color, and the transition is the time to transition to the next color in milliseconds.

Size warn limit If the size (in bytes) of an attachment added to a new email is larger than *Size warn limit*, a warning will be shown to warn the user that the email will be large. This setting is only used when sending encrypted email from the BlackBerry smartphone.

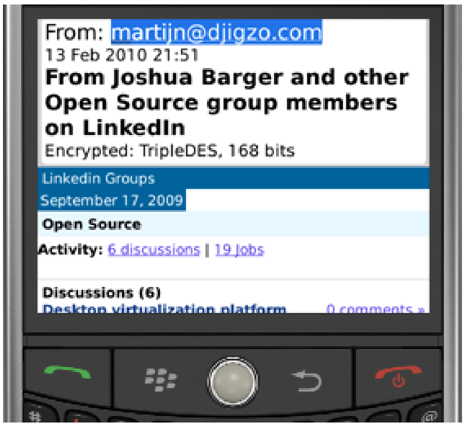
2.4 Reading encrypted email

Encrypted email is stored in the BlackBerry mail application inbox just like normal non-encrypted email. Whether or not the message is automatically decrypted when the user opens the message depends on the size of the encrypted message.

Messages smaller than 64KB will be automatically decrypted when opened (figure 10 shows an HTML message which was encrypted with 3DES). Messages larger than 64KB are not automatically delivered to the BlackBerry smartphone and should be manually opened by the user by selecting *Open Attachment* from the context menu. The message will then be downloaded and opened.

Attachments that should be manually opened can be recognized by the attachment named “attachment.smime” (see figure 11). The body of the message containing the encrypted “attachment.smime” is based on the *BB add-on* template (see the Templates section in the Ciphermail Administration Guide for more information).

Key Store password Depending on the selected *Private key security level* a password must be entered when the message is decrypted with a private key (see figure 12). Depending on the settings, the Key Store password will

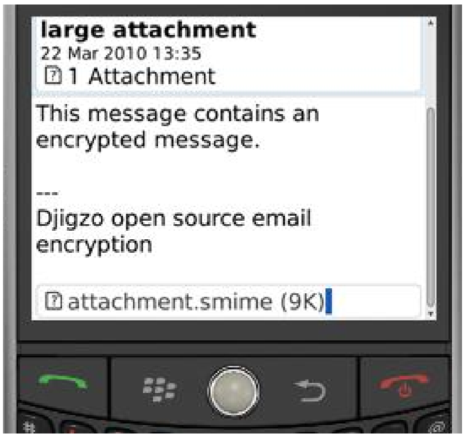


From: martijn@djigzo.com
13 Feb 2010 21:51
From Joshua Barger and other Open Source group members on LinkedIn
Encrypted: TripleDES, 168 bits

Linkedin Groups
September 17, 2009
Open Source
Activity: 6 discussions | 19 Jobs

Discussions (6)
Desktop virtualization platform 0 comments »

Figure 10: Encrypted HTML message



large attachment
22 Mar 2010 13:35
1 Attachment

This message contains an encrypted message.

Djigzo open source email encryption

attachment.smime (9K)

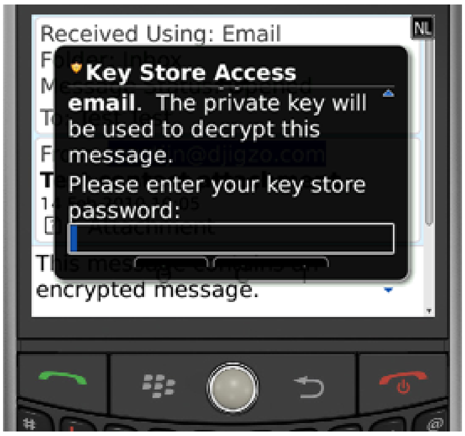
Figure 11: S/MIME attachment

be cached for some time. For more information see *synchronization options* in section 2.2.2.

Suitable Private Key not found If a message is encrypted, but the BlackBerry smartphone cannot find the correct private key to decrypt the message with, a warning message will be shown. For more information on how to find out which certificates were used for encryption see Appendix C.

2.4.1 Attachments

Encrypted messages can contain attachments. The complete message, including any attachment, is encrypted. Ciphermail for BlackBerry allows attachments to be opened and saved. Only attachments for which a content handler is registered can be opened (for example .doc and .xlt files will be opened with *Documents to Go*). Attachments are shown at the bottom of the email (see figure 13). Attachments can be opened by clicking the attachment. Attachments



Received Using: Email

Key Store Access

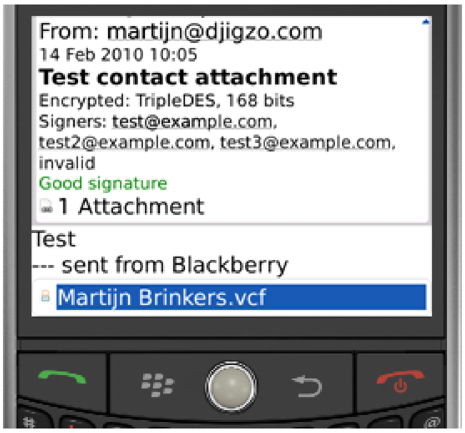
email. The private key will be used to decrypt this message.

Please enter your key store password:

encrypted message.

Figure 12: Key Store password

can be saved by selecting the attachment and selecting *Save Attachment* from the context menu. A save-as popup screen will be opened (see figure 14).



From: martijn@djigzo.com
14 Feb 2010 10:05
Test contact attachment
Encrypted: TripleDES, 168 bits
Signers: test@example.com, test2@example.com, test3@example.com, invalid
Good signature
1 Attachment

Test
--- sent from Blackberry

Martijn Brinkers.vcf

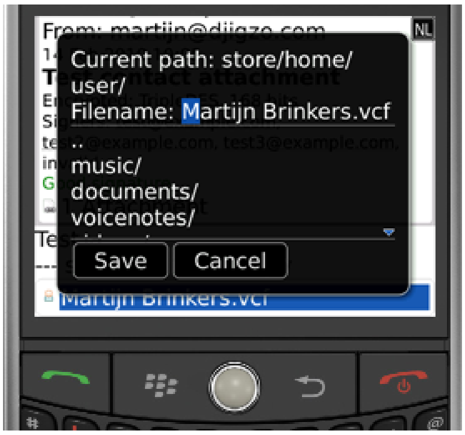
Figure 13: Message with attachment and Good signature.

2.4.2 Signature info

If a message is digitally signed, a signature status line is added to the header section. If the signature is valid, i.e. signed with a trusted certificate and the message is not altered after signing, the signature status line will show “Good signature” in green color (see figure 13). If the signature is invalid the signature status line will show “Bad signature” in red color (see figure 15).

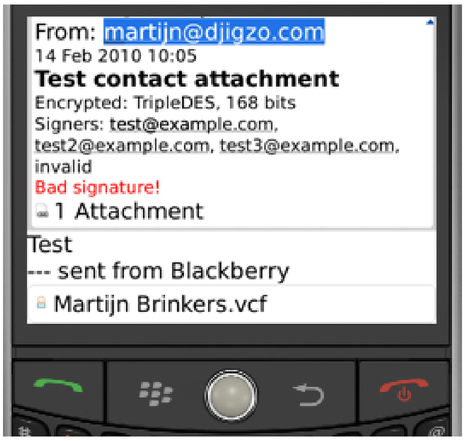
Invalid signature A signature can be invalid for various reasons:

- The signing certificate is not trusted because the root or intermediate certificate is not trusted.



Current path: store/home/user/
Filename: Martijn Brinkers.vcf
..
music/
documents/
voicenotes/

Figure 14: Save attachment



From: martijn@djigzo.com
14 Feb 2010 10:05
Test contact attachment
Encrypted: TripleDES, 168 bits
Signers: test@example.com, test2@example.com, test3@example.com, invalid
Bad signature!
1 Attachment

Test
--- sent from Blackberry

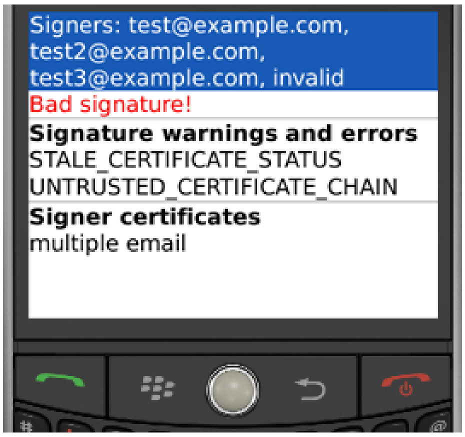
Martijn Brinkers.vcf

Figure 15: Bad signature

- The signing certificate has been revoked.
- The message was altered after signing (message has been tampered).
- The signing certificate is not valid for signing (i.e. the key usage does not allow signing or non-repudiation).
- The signing certificate is not valid for S/MIME (i.e. the extended key usage does not allow email protection).
- The signature is invalid for other reasons (unsupported algorithm, message corruption during transport etc.).

Signature info More information about the signature can be obtained/viewed by selecting the menu option *Signature info*. The signature information screen shows information about which certificate was used for signing and if the signature was invalid why it was invalid (figure 16 for example shows that the signature was invalid because the certificate chain is not trusted).

Certificate details can be viewed by clicking the signing certificate. The certificate details popup screen provides all the details of the certificate like *Subject*, *Issuer*, *Email* etc. (see figure 17).



Signers: test@example.com, test2@example.com, test3@example.com, invalid

Bad signature!

Signature warnings and errors

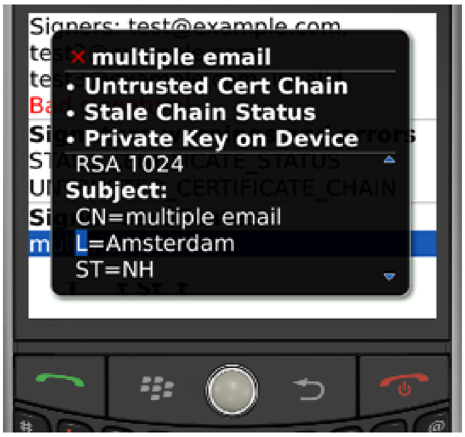
STALE_CERTIFICATE_STATUS

UNTRUSTED_CERTIFICATE_CHAIN

Signer certificates

multiple email

Figure 16: Signature information



multiple email

- **Untrusted Cert Chain**
- **Stale Chain Status**
- **Private Key on Device**

RSA 1024

Subject:

CN=multiple email

L=Amsterdam

ST=NH

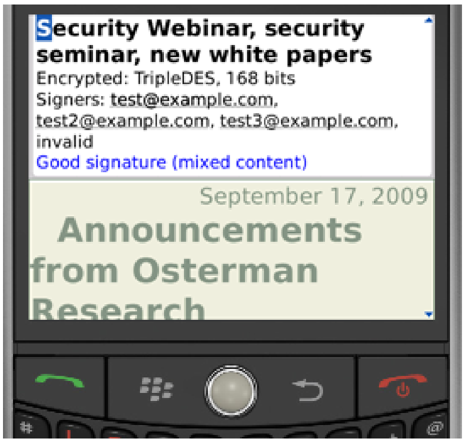
Figure 17: Certificate details

Importing the signing certificate In most cases, when digitally signing a message, S/MIME clients add all signing certificates to the signature 'blob'. Ciphermail for BlackBerry can extract these certificates and import them into the BlackBerry certificate store by selecting the menu item *Import Certificates*. The BlackBerry smartphone asks for the key store password to confirm the import. Importing the certificates from the signature can be helpful when the signature is invalid because the signing certificate is not trusted.

By importing all certificates and explicitly trusting the complete certificate chain, the signing certificate can be made trusted (see 2.6 for more information on managing certificate trust).

External images Sometimes, HTML emails refer to external images. External images are not automatically downloaded by Ciphermail for BlackBerry, mainly because *a)* downloading external images can reveal the recipient[6] *b)* When a message is signed it's not clear which part of the message is signed and which part is not signed because only the image URLs are signed, not the actual image content.

Messages can be downloaded by selecting *Get Images* from the menu. If a message is digitally signed and the signature is valid the signature status line is changed from "Good signature" to "Good signature (mixed content)" to indicate that some parts of the message are not digitally signed (see figure 18).



Security Webinar, security seminar, new white papers
Encrypted: TripleDES, 168 bits
Signers: test@example.com, test2@example.com, test3@example.com, invalid
Good signature (mixed content)

September 17, 2009
Announcements from Osterman Research

Figure 18: Mixed content

2.5 Sending secure email

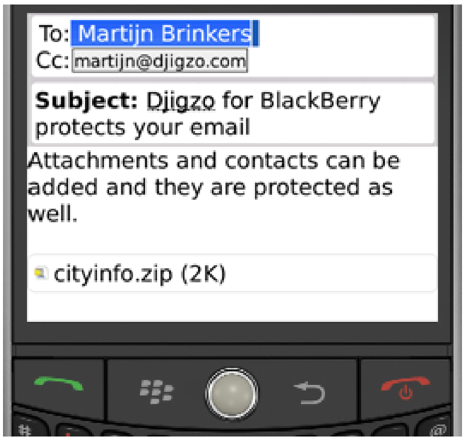
Before email can be securely sent with Ciphermail for BlackBerry the following settings must be configured: *From*, *Sign cert*, *Enc. cert* and *Relay email* (see 2.3.1). If one of these settings is missing, the message cannot be sent and a warning will be shown.

A secure message sent by Ciphermail for BlackBerry is relayed to a Ciphermail gateway via an encrypted S/MIME tunnel. The Ciphermail gateway then forwards the message to the final recipient. Whether or not the forwarded message is encrypted depends on the gateway settings (see *Sending S/MIME encrypted email* on page 5 for more information).

A new secure email can be created by selecting *Compose Secure Email* from the menu. A secure reply to a secure message can be created by selecting *Reply Secure* or *Reply To All Secure* from the menu. A secure email can be securely forwarded by selecting *Forward Secure* from the menu. The secure compose screen allows files and contacts to be attached (see figure 19).

There are three different ways to securely send a message: *Send*, *Send Encrypted* and *Send As PDF/SMS* (see figure 20). It should be noted that

[6] A sender can give a message a URL which uniquely identifies the message. The sender can detect if, when and from where the recipient reads the message by logging all details when the image is downloaded.



To: Martijn Brinkers
Cc: martijn@djigzo.com

Subject: Djigzo for BlackBerry protects your email

Attachments and contacts can be added and they are protected as well.

cityinfo.zip (2K)

Figure 19: Composing a secure email

in all of the three cases all email between the BlackBerry smartphone and the Ciphermail gateway is encrypted by means of an S/MIME tunnel. The difference between the three ways of securely sending a message is how the Ciphermail gateway forwards the message to the final recipient.

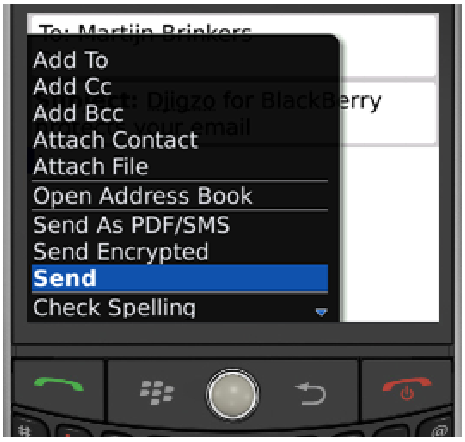


Figure 20: Sending secure email

Send With the Send option, the message is securely “S/MIME tunneled” to the Ciphermail gateway. The Ciphermail gateway then forwards the message to the final recipient. How the Ciphermail gateway handles the message depends on the Ciphermail gateway settings. If, for example, the recipient has encryption enabled and a valid S/MIME certificate is available, the email will be encrypted.

Send Encrypted The *Send Encrypted* option is similar to the *Send* option. The only difference is that the *Enc. trigger* keyword is appended to the subject of the message (see the Enc. trigger option on page 11). The Send Encrypted option requires that the Ciphermail gateway is setup to allow the *Subject trigger* (see the Ciphermail Administration Guide for more information).

The Send Encrypted option should be used if the sender of the message requires that the message sent to the final recipient is encrypted by the Ciphermail gateway. If the message cannot be encrypted by the Ciphermail gateway, the message will not be sent and the sender will be notified.

Send As PDF/SMS The *Send As PDF/SMS* option is similar to the *Send Encrypted* option. The only difference is that the mobile telephone number of the recipient is appended to the subject.

Sending a message with *Send As PDF/SMS* instructs the Ciphermail gateway to send the message as an encrypted PDF. The password for the PDF is delivered to the recipient via an SMS Text message. The SMS Text message with the password will be sent to the recipients telephone number specified in the recipients BlackBerry addressbook account.

If the recipient's addressbook account does not contain a telephone number a warning message will be shown and the message won't be sent. Only one recipient for the message is allowed when sending a message with *Send As PDF/SMS*. If multiple recipients are specified a warning message will be shown and the message won't be sent.

The Send As PDF/SMS option requires that the Ciphermail gateway is setup to allow sending SMS Text messages and that the telephone number be set on the subject of the message (see the Ciphermail Administration Guide for more information).

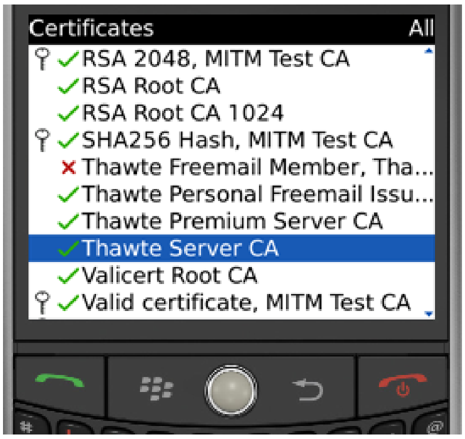
2.6 Certificate management

Even though most certificate management should be done on the Ciphermail gateway sometimes certificates should be locally managed on the BlackBerry smartphone. For example when validating digitally signed messages, Ciphermail for BlackBerry uses the local certificate store to check whether the signing certificate is trusted. If a certificate is not locally trusted Ciphermail for BlackBerry cannot validate the signature (see 2.4.2 for more information).

A BlackBerry smartphone contains a local certificate store. The certificate store can be managed by opening the certificate manager options screen (Options→Security Opions→Certificates). Certificates with an associated private key have a key icon in the first column (see figure 21). Certificates which are not valid (not trusted by a root, expired etc.) are shown with a red cross.

The following certificate stores are available: *My Certificates*, *Others Certificates*, *CA Certificates* and *Root Certificates* (see figure 22). By selecting one of the available menu options a specific certificate store can be opened. The *My Certificates* store contains all the certificates with a private key.

Certificate details By clicking a certificate the *certificate details* popup dialog will be shown.



Certificates All

✓ RSA 2048, MITM Test CA
✓ RSA Root CA
✓ RSA Root CA 1024
✓ SHA256 Hash, MITM Test CA
× Thawte Freemail Member, Tha...
✓ Thawte Personal Freemail Issu...
✓ Thawte Premium Server CA
✓ Thawte Server CA
✓ Valicert Root CA
✓ Valid certificate, MITM Test CA

Figure 21: Certificate manager

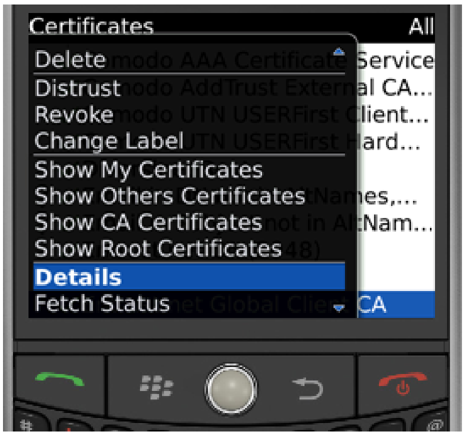
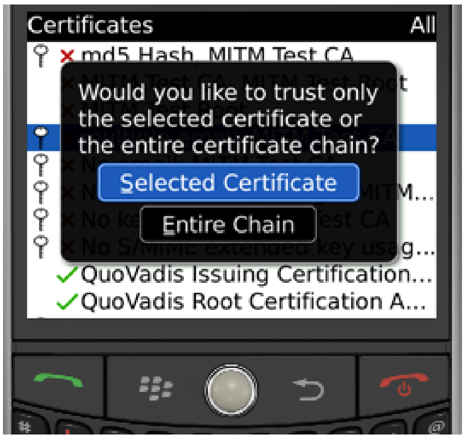


Figure 22: Certificate manager menu options

Certificate trust If a certificate is not trusted - for example, because the root certificate is not trusted - the certificate can be manually set to "trusted" by selecting *Trust* from the context menu. If a non-root certificate is manually set to trusted a popup dialog will be shown asking the user whether the complete certificate chain or only the selected certificate should be trusted (see figure 23). Select *Entire Chain* if the root and intermediate certificates should also be trusted.

Change Security Level The security level of the private key associated with a certificate can be changed by selecting *Change Security Level* from the context menu (see Synchronization Options on page 7 for more information on the different security levels).



Certificates All

✗ md5 Hash MITM Test CA

Would you like to trust only the selected certificate or the entire certificate chain?

✓ QuoVadis Issuing Certification...

✓ QuoVadis Root Certification A...

Figure 23: Certificate Trust

3 Gateway configuration

Ciphermail for BlackBerry requires a fully functional Ciphermail gateway. This guide only explains how to configure a Ciphermail gateway to be used with Ciphermail for BlackBerry. For more information on how to setup a Ciphermail gateway see the *Ciphermail Administration Guide*.

3.1 Infrastructure

As explained in section 2, email must be handled by a Ciphermail gateway before being sent to a BlackBerry smartphone. Where exactly a Ciphermail gateway should be placed within the email infrastructure depends on a number of factors, like whether the company is running it's own SMTP server and whether the BlackBerry devices retrieve their email from the companies internal *POP3*/*IMAP* server or from some other external server (for example Gmail or the BIS email account provided by your telecom provider).

Three scenario's: The following three scenario's are most common:

1. The company runs its own email server. The BlackBerry retrieves its email from an external server (*POP3*, *IMAP* or BIS email account).
2. The company runs its own email server. The BlackBerry retrieves its email from an internal server (*POP3*, *IMAP*).
3. The company does not run its own email server. The BlackBerry retrieves its email from an external server (*POP3*, *IMAP* or BIS email account).

Scenario 1: Company email server, external mailbox With this setup it is assumed that the companies email server forwards all incoming email to an external email address (for example a Gmail, BIS or some other external email address). Email is received on the company's domain and forwarded to the

BlackBerry email address. The BIS infrastructure then pushes the email to the BlackBerry smartphone. The Ciphermail gateway should be placed between the internal email server and the Internet (see figure 24). Because all email is sent via the Ciphermail gateway all email sent to the BlackBerry email address can be encrypted.

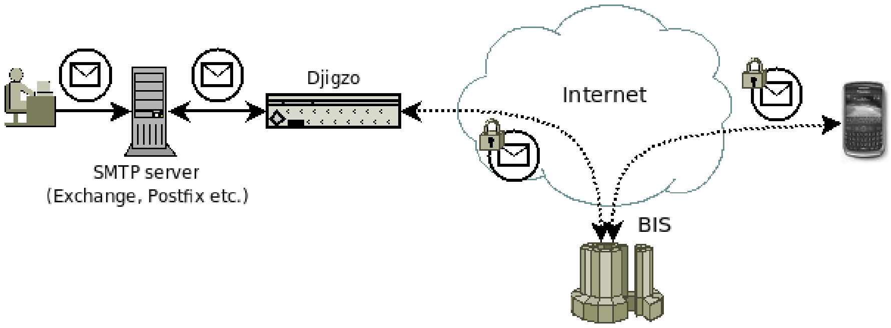


Figure 24: Company email server, external mailbox

Scenario 2: Company email server, internal mailbox With this setup email is received on the company's domain and placed in the user's mailbox (for example on Exchange). The user's BlackBerry BIS account is setup to retrieve email via *POP3* or *IMAP* directly from the companies email server.

Any email must be handled by Ciphermail before the message can be delivered to the BlackBerry smartphone. Ciphermail should therefore periodically extract all email from the local mailbox (using Fetchmail), encrypt the email and then deliver the encrypted email to the secondary secure mailbox. The secure mailbox now only contains encrypted email. BIS now retrieves the email from the secure mailbox and sends the encrypted message to the BlackBerry smartphone (see figure 25). The emails, after being handled by the Ciphermail gateway, should be stored in a different mailbox than the non-encrypted emails. This setup therefore requires that the user has a secondary mailbox (which we will call the "secure mailbox") which only stores the encrypted email.

The procedure:

1. User sends a message to an internal recipient.
2. The message is delivered to the recipient's mailbox.
3. The Ciphermail gateway retrieves the message from the recipients mailbox using Fetchmail (The Ciphermail Virtual Appliance has Fetchmail built-in).
4. The Ciphermail gateway encrypts the message with the public certificate of the BlackBerry recipient.
5. The encrypted message is delivered to the secure mailbox of the recipient.

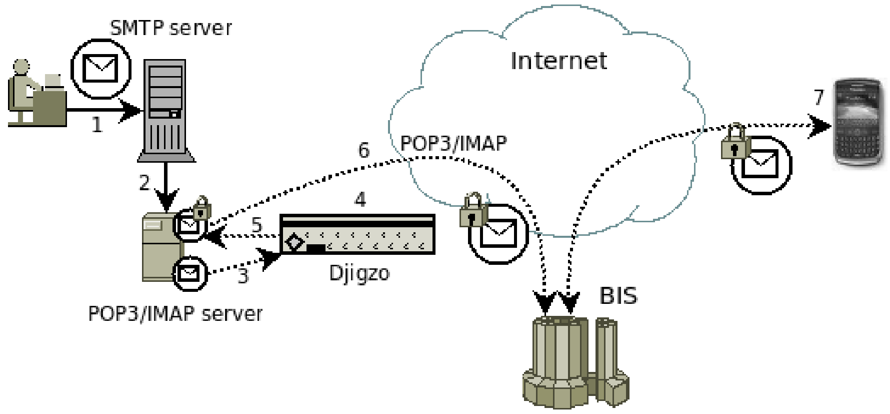


Figure 25: Company email server, internal mailbox

6. BIS retrieves the encrypted message from the secure mailbox.
7. The encrypted message is delivered to the BlackBerry smartphone.

Note: the initial message (step 1) can already be S/MIME encrypted with the public certificate of the BlackBerry recipient. The Ciphermail gateway does not need to decrypt the message. It only needs to rewrite a header (see Appendix A for more information).

The *POP3*/*IMAP* server need not be an internal server. An external server (for example Gmail) can be used as well. However, if an external server is used email delivered to the external *POP3*/*IMAP* server should be secured as well.

Scenario 3: No email server, external mailbox This setup is required when the company (or user) does not have it's own email server. Email is received by an external server and BIS retrieves the email from the external server and sends it to the BlackBerry smartphone. This setup is more or less similar to Scenario 2.

Any email must be handled by the Ciphermail server before the message can be delivered to the BlackBerry smartphone. Ciphermail should therefore periodically extract all email from the remote mailbox (using Fetchmail), encrypt the email and then deliver the encrypted email to the secondary remote secure mailbox. Thus, the secure mailbox only contains encrypted email. BIS now retrieves the email from the remote secure mailbox and sends the encrypted message to the BlackBerry smartphone (see figure 26). Because the emails handled by the Ciphermail gateway (i.e. the encrypted emails) should be stored in a different mailbox than the non-encrypted emails this setup requires that the user has a secondary mailbox (which we will call the “secure mailbox”) which only stores the encrypted email.

The procedure:

1. User sends a message to an external recipient.

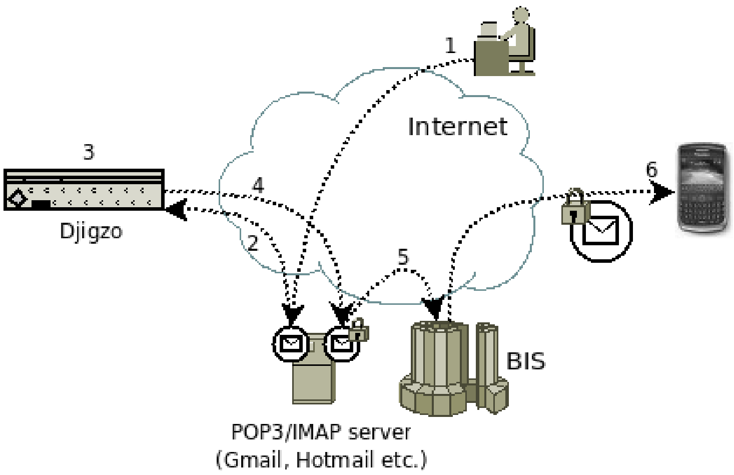


Figure 26: No email server, external mailbox

2. The Ciphermail gateway retrieves the message from the recipients mailbox using Fetchmail (The Ciphermail Virtual Appliance has Fetchmail built-in).
3. The Ciphermail gateway encrypts the message with the public certificate of the BlackBerry recipient.
4. The encrypted message is delivered to the secure external mailbox of the recipient.
5. BIS retrieves the encrypted message from the secure mailbox.
6. The encrypted message is delivered to the BlackBerry smartphone.

Note: it may happen that the initial message (step 1) is already S/MIME encrypted with the public certificate of the BlackBerry recipient. The Ciphermail gateway does not need to decrypt this message, it only needs to rewrite one of the message headers (see Appendix A for more information).

A secondary mailbox is required for the encrypted email. If the BlackBerry user is using a BIS email account exclusively (i.e. external senders send their email to the BIS email address) an new email account should be created to which external sender should send their email to. The Ciphermail server will then deliver the encrypted email to the BIS account.

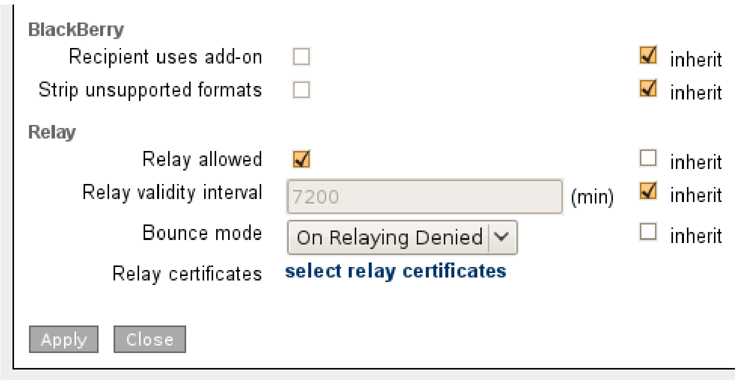
Pros and cons The advantage of scenario 1 is that all outgoing email can be encrypted when needed. Scenario 1 is also the most scalable scenario as it supports almost unlimited number of accounts. The disadvantage is that Ciphermail must be placed within the current email infrastructure. The main advantage of both scenarios 2 and 3 is that email for the BlackBerry can be encrypted without requiring structural changes to the email infrastructure. The disadvantage of scenario 2 and 3 is that it's not highly scalable. Fetchmail should only be used for a limited number of accounts.

3.1.1 Fetchmail

The Ciphermail Virtual Appliance has built-in Fetchmail support. Fetchmail can be used to retrieve email from remote *POP3*, *IMAP* servers and forward the email to different email addresses via the Ciphermail gateway. Ciphermail allows the administrator to configure Fetchmail via a web based configuration page. The built-in Fetchmail support can be used with scenario 2 and 3. See the *Ciphermail administration guide* for more information.

3.2 BlackBerry Settings

Ciphermail gateway settings specific for Ciphermail for BlackBerry are: *Recipient uses add-on*, *Strip unsupported formats* and *Relay* settings (see figure 27).



BlackBerry

Recipient uses add-on □ ☑ inherit

Strip unsupported formats □ ☑ inherit

Relay

Relay allowed ☑ □ inherit

Relay validity interval 7200 (min) ☑ inherit

Bounce mode On Relaying Denied □ inherit

Relay certificates select relay certificates

Figure 27: Ciphermail Gateway BlackBerry Settings

Recipient uses add-on As explained in section 2 and appendix A, S/MIME messages are by default blocked by BIS. S/MIME messages require some changes to the headers to prevent BIS from blocking the S/MIME message. By selecting *Recipient uses add-on* the Ciphermail gateway is instructed to apply the required changes when an S/MIME message is sent to the BlackBerry recipient.

Please be aware that the S/MIME message can no longer be read by standard S/MIME email clients after the required changes. Therefore, the *Recipient uses add-on* setting should therefore only be enabled for BlackBerry accounts.

Strip unsupported formats The BlackBerry smartphone has built-in handlers for some types of attachments like images, sounds, Office documents using "Documents to Go" etc. Not all attachments however can be handled by these handlers.

If *Strip unsupported formats* is checked, unsupported attachments are removed from the message before the Ciphermail gateway digitally signs and encrypts the message. This saves bandwidth and costs, especially when the user does not have an unlimited data plan[7]. If the message is already signed or encrypted the unsupported attachments will not be removed.

3.3 Relay Settings

The Relay Settings are required when encrypted email must be sent with Ciphermail for BlackBerry. As explained in section *Sending S/MIME encrypted email* on page 5, encrypted email sent with Ciphermail for BlackBerry is delivered via the BlackBerry infrastructure to the Ciphermail gateway. The Ciphermail gateway then forwards the message to the final recipient.

The Ciphermail gateway contains user specific preferences that control whether a sender is allowed to relay messages. The following user relay preferences can be set: *Relay allowed*, *Relay validity interval*, *Bounce mode* and *Relay certificates*.

Relay allowed If false the user is not allowed to relay email even if the correct signature is used. If a user should be able to relay email through the Ciphermail gateway, *Relay allowed* should be enabled for the user.

Relay validity interval A message sent with Ciphermail for BlackBerry is time-stamped. If a message is older then *Relay validity interval* (in minutes) the message is not accepted. By default a relay message is valid for 5 days (7200 minutes).

Bounce mode There are various reasons why an email is not accepted for relay by the Ciphermail gateway. For example, the digital signature is corrupt, the certificate is not an acceptable relay certificate, the relay message has expired (see *Relay validity interval*), or the sender is not allowed to relay (see *Relay allowed*). How the Ciphermail gateway handles invalid relay messages depends on the *Bounce mode*. There are three Bounce modes: *Never*, *On Relaying Denied* and *On Invalid Recipient*.

Never bounce mode will never result in a bounced message. With bounce mode *On Relaying Denied* the relay message will bounce when: *a)* relaying is not allowed, *b)* the message has expired or *c)* the recipient is not a valid email address. With bounce mode *On Invalid Recipient* a relay message will only be bounced if the recipient is not a valid email address.

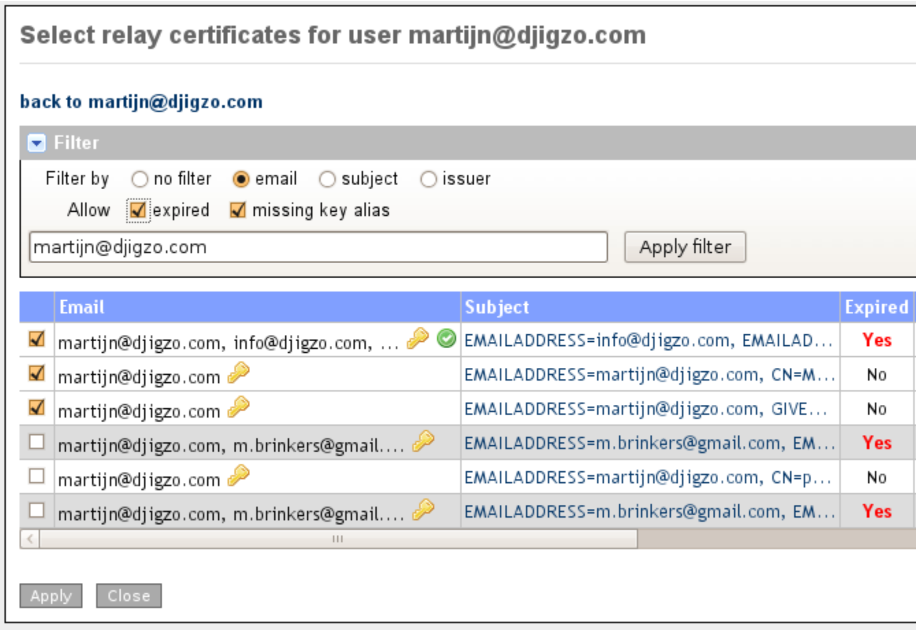
The bounce message is not the relay message itself, but rather a notification message containing the reason for the bounce.

Relay certificates To make sure that only authenticated users can relay email via the Ciphermail gateway all email sent by Ciphermail for BlackBerry must be digitally signed. The Ciphermail gateway will only relay the message when the

[7] Removing unsupported attachments also helps to keep the total message size below 64KB (see section 2 for more information).

signature is correct and the message is digitally signed with the correct certificate for the sending user (the *Relay certificate* is used to authenticate the user).

Relay certificates that are valid for a user (or domain) can be set by clicking *select relay certificates* (see figure 27). This opens the *Select relay certificates* page for the user or domain (see figure 28).



Select relay certificates for user martijn@djigzo.com

back to martijn@djigzo.com

Filter

Filter by ○ no filter ● email ○ subject ○ issuer

Allow ☑ expired ☑ missing key alias

martijn@djigzo.com

	Email	Subject	Expired
☑	martijn@djigzo.com, info@djigzo.com, ...	EMAILADDRESS=info@djigzo.com, EMAILAD...	Yes
☑	martijn@djigzo.com	EMAILADDRESS=martijn@djigzo.com, CN=M...	No
☑	martijn@djigzo.com	EMAILADDRESS=martijn@djigzo.com, GIVE...	No
□	martijn@djigzo.com, m.brinkers@gmail....	EMAILADDRESS=m.brinkers@gmail.com, EM...	Yes
□	martijn@djigzo.com	EMAILADDRESS=martijn@djigzo.com, CN=p...	No
□	martijn@djigzo.com, m.brinkers@gmail....	EMAILADDRESS=m.brinkers@gmail.com, EM...	Yes

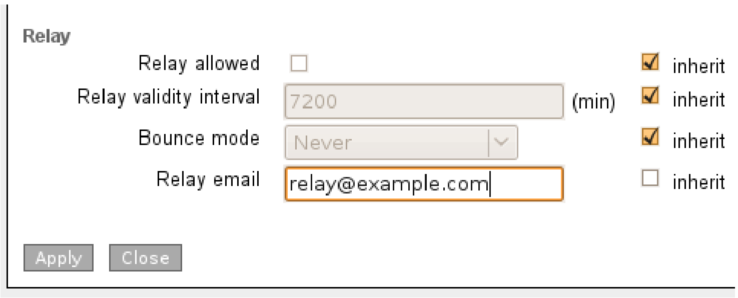
Figure 28: Relay Certificate Selection

A relay certificate selected for a user or domain should be the same certificate that is selected as the *Sign cert* certificate in the Ciphermail for BlackBerry settings (see *Sign cert* settings on page 9). If the relay certificate is not the same as the signing certificate the Ciphermail gateway will not relay the message. It is advised to give each user their own relay certificate instead of setting a relay certificate for a domain.

Relay email address As explained in section *Sending S/MIME encrypted email* on page 5, encrypted email sent with Ciphermail for BlackBerry is delivered via the BlackBerry infrastructure to the Ciphermail gateway. The Ciphermail gateway then forwards the message to the final recipient. Because the relay message is delivered to the Ciphermail gateway using regular (although encrypted) email the Ciphermail gateway should have a special relay email address on which it listens for relay messages.

The relay email address should be specified on the advanced relay global settings page (see figure 29). We advise you to use an email address which is only used for relay messages. The relay email address should be a real email address for which email can be received (either in a mailbox or by forwarding it to another email address). Relay messages that are not relayed because they are not valid as relay messages, as well as relay messages that are not bounced are delivered to the relay account[8].

The relay email address should be the same email address as the relay address set on the Ciphermail for BlackBerry settings screen (see *Relay email* setting on page 10). Ciphermail for BlackBerry sends encrypted email to this address.



Relay

Relay allowed	□		☑ inherit
Relay validity interval	7200	(min)	☑ inherit
Bounce mode	Never		☑ inherit
Relay email	relay@example.com		□ inherit

Figure 29: Global Relay Settings

[8] A relay message is decrypted before the signature is checked. If a relay message is invalid and not bounced the undecrypted relay message will be delivered to the relay account. The relay account should therefore be protected.

A BIS and S/MIME messages

This appendix will briefly explain why S/MIME messages by default are blocked by BIS and what changes are required to an encrypted S/MIME message to allow BIS to forward the message to a BlackBerry smartphone. The information in this appendix is only for background information and is not required for running Ciphermail for BlackBerry. This appendix can be skipped if the reader is not interested in the technical details of why an external server is required.

An S/MIME message is an email message to which the encrypted message is attached as a binary attachment. The encrypted attachment can be recognized by S/MIME capable email clients because the `Content-Type` of the message is set to `application/pkcs7-mime`.

Example of an encrypted message:

```
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type=enveloped-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message

MIAGCSqGSIb3DQEHA6CAMIACAQAxggETMIIBDwIBADB4MGQxCzAJB
....
HiXe+Yq5w/kpqsbBDXOkBNyNlFydyhPewFvqbh4AAAAAAAAAAAAA
```

Even though a BlackBerry smartphone can handle S/MIME messages, BIS blocks all attachments it cannot handle. This includes the attachment used by S/MIME messages. This means that all S/MIME email messages sent to a BlackBerry smartphone are blocked by BIS.

There are two workarounds that force BIS to forward the attachment to the BlackBerry. The first workaround is to prefix the attachment filename with `x-rimdevice`. You can, for example, rename `smime.p7m` to `x-rimdevicesmime.p7m`. The second workaround is to rename the extension to something different than .p7m (for example, you can rename the attachment to .smime). Additionally, the content-type of the message has to be changed from S/MIME to a general binary content-type because according to this article S/MIME messages are never sent to the BlackBerry.

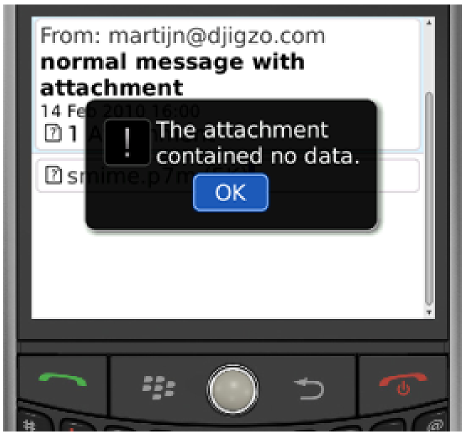
> Note: S/MIME (Secure Multipurpose Internet Mail Extensions) attachments are not delivered to the BlackBerry smartphone, regardless of the x-rimdevice prefix.

To make sure that the S/MIME attachment is delivered, the content-type of the message has to be changed from application/pkcs7-mime to application/octet-stream. Attachments prefixed with x-rimdevice are immediately delivered to the BlackBerry smartphone whereas attachments renamed to .smime are not directly delivered (they should be downloaded on demand). The size of attachments prefixed with x-rimdevice however is limited to 64KB. Attachments larger than the 64KB should therefore be renamed to .smime. S/MIME messages that are larger than 64KB should therefore be downloaded “on demand”. Attachments up to 5MB can be received by the BlackBerry smartphone.

The Ciphermail Email Encryption Gateway is capable of modifying the required headers to make sure that the S/MIME message is delivered to the BlackBerry smartphone.

The S/MIME message won't open If an S/MIME message is sent to the BlackBerry smartphone without the required changes, the S/MIME attachment will be blocked by BIS (see previous explanation).

Even though it appears that the S/MIME attachment is not empty (i.e. the reported attachment size seems to be correct) when accessed, the attachment is actually empty. If the attachment is manually opened a warning message reporting that the attachment contains no data will be shown (see figure 30).



From: martijn@djigzo.com
normal message with attachment
14 Fe 2010 16:00

smime.p7m

The attachment contained no data.

Figure 30: Empty S/MIME attachment

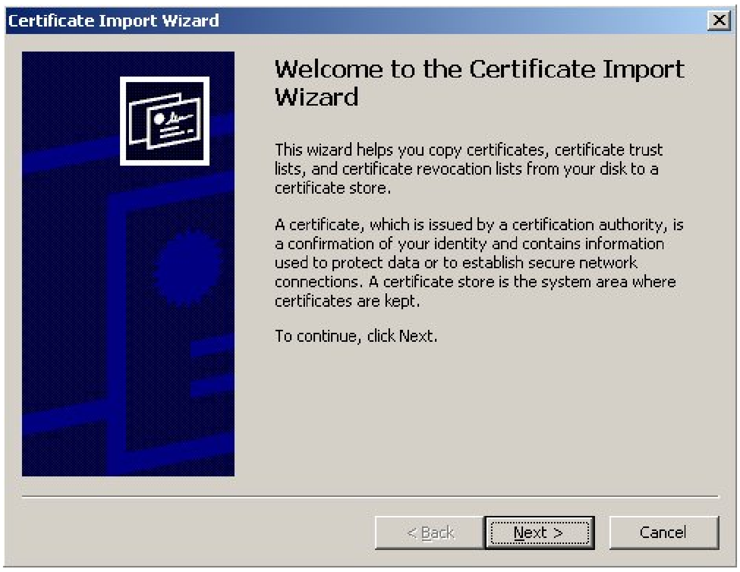
B Importing a .pfx file

A .pfx file contains certificates and keys. The certificates and keys can be imported into Windows with the following procedure:

1. Double-click the .pfx file to start the *Certificate Import Wizard*.
2. Step through the *Certificate Import Wizard* (leave the default values in place).
3. When asked for the private key password, enter the .pfx password. Make sure that *Mark this key as exportable*. . . is checked!
4. Press Next for all pages.
5. On the final page, if asked to accept the trusted root certificate select *Yes*.

The above steps will now be explained in more detail.

Double-click the.pfx file. The *Certificate Import Wizard* will be started (see figure 31).
Press Next until the password entry page is reached (see figure 32).



Certificate Import Wizard

Welcome to the Certificate Import Wizard

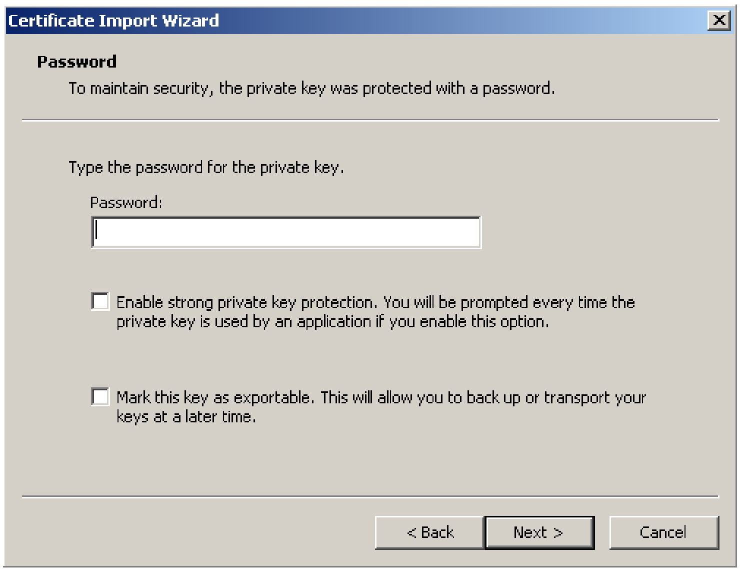
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 31: Certificate Import Wizard

Note: make sure the *Mark this key as exportable. . .* checkbox is checked otherwise the key cannot be exported to the BlackBerry smartphone!



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

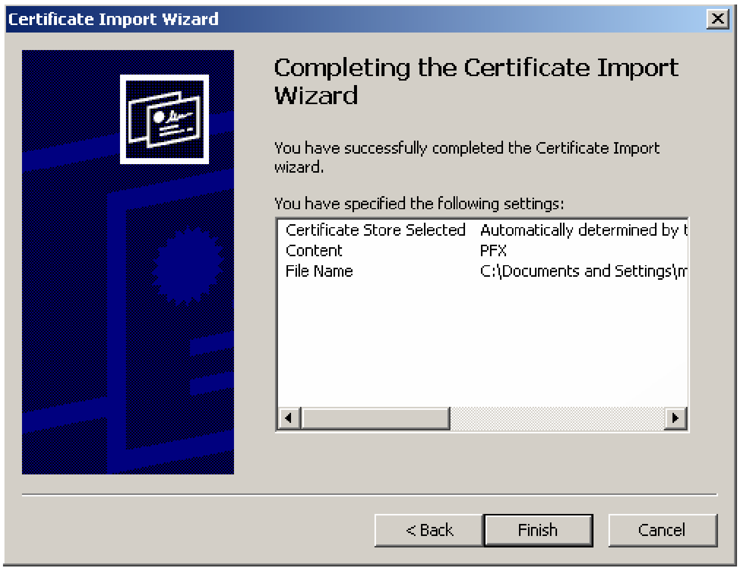
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

Figure 32: Certificate Import Wizard enter password

Now, click the *Next* button and on the next pages leave the defaults until the *Completing the Certificate Import Wizard* page is reached (see figure 33). On the final page, click *Finish* to start importing both the certificate and private key.

The pfx file not only contains the end-user certificate and private key, some-



Completing the Certificate Import Wizard

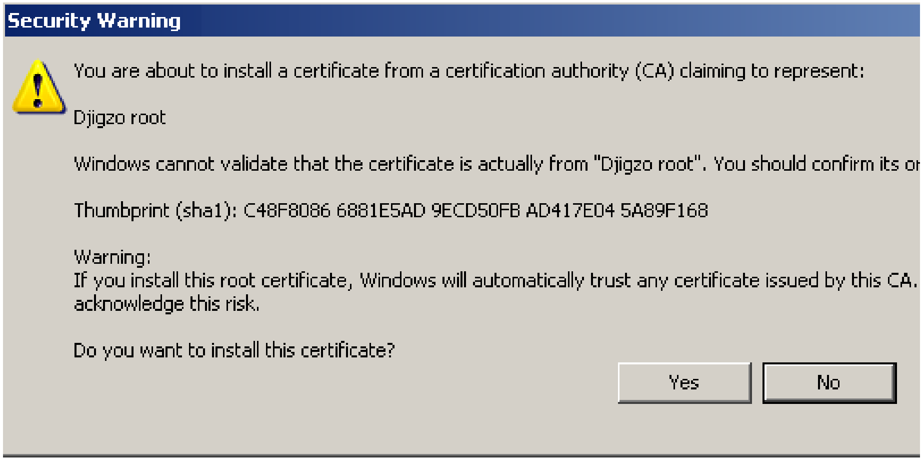
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Documents and Settings\m

Figure 33: Certificate Import Wizard finish

times the root and intermediate certificate are included as well. The import wizard will also try to import the root and intermediate certificate. Windows asks for permission when importing a root certificate (see figure 34).



You are about to install a certificate from a certification authority (CA) claiming to represent:

Djigzo root

Windows cannot validate that the certificate is actually from "Djigzo root". You should confirm its or

Thumbprint (sha1): C48F8086 6881E5AD 9ECD50FB AD417E04 5A89F168

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. acknowledge this risk.

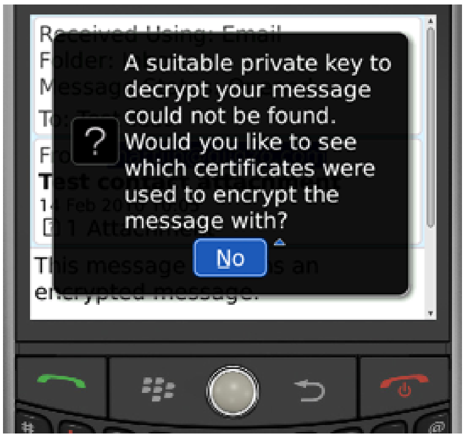
Do you want to install this certificate?

Figure 34: Certificate Import Wizard root import warning

Click *Yes* to accept the root certificate but only if the root certificate comes from a trusted source. Importing the root certificate is not required. However if the root certificate is not installed it can happen that digitally signed email received on the BlackBerry cannot be validated (i.e. a “Bad signature” warning will be shown).

C Suitable Private Key not found

If a message is encrypted but the BlackBerry smartphone does not have the correct private key for decryption, a warning message will be shown (see figure 35). By selecting *Yes* a list of certificate identifiers will be shown (see figure 36).



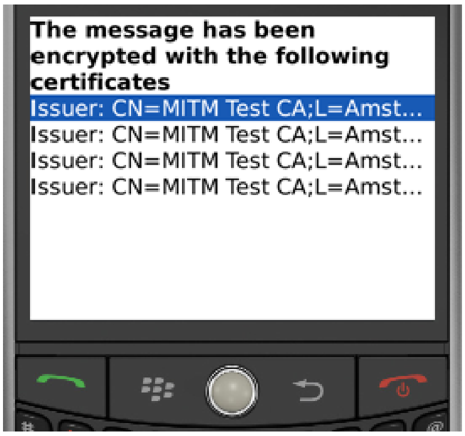
A suitable private key to decrypt your message could not be found. Would you like to see which certificates were used to encrypt the message with?

Figure 35: Suitable Private Key not found

The details of the certificate identifier can be shown by clicking the list item. The *CMS Entity Identifier* screen provides all the available information to identifying the certificates used for encryption. The following items are shown: *Issuer*, *Serial Nr* and *Subj. Key Id*.

The *Issuer* is the issuer of the certificate and the *Serial Number* is the serial number of the certificate. An issuer should never use a serial number twice. The serial number in combination with the Issuer should uniquely identify a certificate.

The Subject Key Identifier is another way to uniquely identify the certificate. In most cases however Issuer and Serial Number is used instead of Subject Key Identifier and Subject Key Identifier is therefore almost always blank.



The message has been encrypted with the following certificates

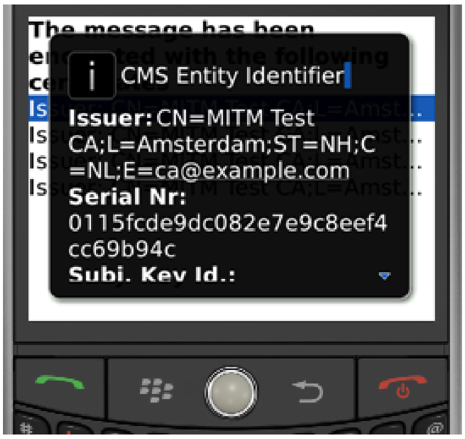
Issuer: CN=MITM Test CA;L=Amst...

Issuer: CN=MITM Test CA;L=Amst...

Issuer: CN=MITM Test CA;L=Amst...

Issuer: CN=MITM Test CA;L=Amst...

Figure 36: Encryption Recipients



CMS Entity Identifier

Issuer: CN=MITM Test CA;L=Amsterdam;ST=NH;C=NL;E=ca@example.com

Serial Nr: 0115fcde9dc082e7e9c8eef4cc69b94c

Subj. Key Id.:

Figure 37: CMS Entity Identifier